

26 DEC 2017



JOUDAH INFO-LINGO TECH Pvt. Ltd.

شركة الجودة لخدمات اللغة والتكنولوجيا الخاصة المحدودة

TRANSLATOR CERTIFICATE

Dr.Abu Mazhar Khalid Siddique

Translated Document: In the Land of Saudi Creativity

Mr. Cheman Shaik

File Reference No: C00357-C00362

I, **Abu Mazhar Khalid Siddique**, translator of **M/S Joudah Info-Lingo-Tech Pvt. Ltd.**, hereby declare that I am competent in the English and Arabic languages, and certify that I have translated the attached document, named above, from Arabic to English to the best of my knowledge and ability.

Signed

26th, December 2017



Dr.Abu Mazhar Khalid Siddique

Doctor of Philosophy in Translation studies

Master of Philosophy in Translation studies

Master in Modern Arabic & Translation studies

Al Alem (The scientist) Arabic Monthly Magazine - Feb 2007

A special interview with an Indian scientist for understanding his thoughts.

In the land of Saudi creativity.

Indian scientist invents the safest encryption system

- **Was the invention made while you were working?**

It is not an on-job or sponsored research. It is the outcome of my leisure time avocation during my weekends, holidays and vacation. The Encryption Technique was invented slightly more than six years back when I was in India.

- **How did you invent this?**

Six years back, when I was a core Java developer in Hyderabad, I developed a great deal of interest in e-commerce. During that period of my career, what had greatly influenced me was the cryptography and information security facet of e-commerce, which has a lot to do with advanced mathematics.

Driven by the curiosity to know how breaking an encrypted message in e-commerce takes more than million years while encryption takes less than a second, I learned the in and out of the discrete mathematics used in encryption algorithms. I got thorough with the theorems and high-funda involved, but eventually identified a shortcoming of the encryption solutions available in the market.

JILT

Head Office: #9-4-131/28, Tombs Road, Tolichowki, Hyderabad-500008, India, Tel: 011-4005146277,
website: www.jilt.co.in, e-mail: info@jilt.co.in

Date 26/12/2017 DOC # C00357

Authorised by: 



I was not satisfied with the single side security that the existing solutions were providing to internet communications where in messages are secured only as long as the private key is kept confidential.

'What if there are dishonest elements inside a business organization revealing the secret bits of information to adversaries or competitors?' - this was a serious question that was mind bogging for me. I was strongly determined to take information security a step further reinforcing the fragile other end of the encryption methodologies applied in e-commerce. Consequently, I came out with the new concept of Absolute Public Key Cryptography ensuring security for e-commerce despite trust-breach attacks by insiders in business enterprises.

Today, e-commerce merchants, e-banking service providers and government organizations are very much worried about protecting their highly sensitive and confidential information from internal agents of competitors and spies of adversaries. Now, they all can coolly relax implementing my encryption. It will make lot of difference in internet-trading of advanced countries like USA where people commit transactions worth millions of Dollars every day and the loss incurred is also as high as \$ 50 billion annually due to identity theft and data breach.

My invention is a cryptographic technic that protects buyers' credit cards, passwords, social security numbers etc.

- **Who inspired you?**

It is a self inspired drive that took off my aspiration to achieve something significant that will be useful to the e-commerce world.

My sustained interest in mathematics since my elementary school days and my sense of its application in real life directed my leisure-time



Research activities towards cryptography and encryption algorithms applied in today's Internet activities.

Though it was my self-inspired initiative, I received ample of support and cooperation from my family.

- **How did you apply for a patent?**

Following my invention, I started searching on the Internet for a person or party who can review and evaluate it. One day I came across the United States Patent & Trademark Office (USPTO), an agency of the US Government that issues patents for qualifying inventors after a rigorous examination. Soon I lodged my patent application in USPTO with the necessary documentation and processing fees. After four years of waiting full of patience, I received their office action reply. After one more year of follow-up with USPTO responding to their queries and addressing their objections, I was issued a patent valid for a period of 17 years. Meanwhile, the research paper was published and presented at the international conference EC2ND held at the University of Glamorgan, U.K, where it was peer reviewed and accepted by the conference committee.

- **Who helped you?**

In fact, I didn't seek any help from others, nor did I come across any one who had a similar interest. I did that alone. Usually, an invention like this comes out with a combined effort of two or three scholars from universities or technology giants or pure R&D institutes.

RSA, a similar algorithm available today in the market was invented in 1976 by three research scholars Rivest, Shamir and Addleman at MIT in the USA. ECC, another similar algorithm was invented in 1985 by Professor Neal Koblitz, a number theorist, and Victor Miller from IBM.



But these algorithms are useful only if there are no bad guys inside the organization.

As soon as I received the patent, I shared the news with my friends. A couple of my close friends, Moidur Rahman and Obaidur Rahman, extended lot of help in taking it to the news media. They have even referred my achievement to an international Indian welfare society (BISWAS), who felicitated me with an appreciation award.

- **What exactly is your invention?**

It is an Encryption Algorithm that protects online buyers' credit card details, and identity credentials such as passwords, social security numbers etc., from hackers and eavesdroppers supported by internal dishonest people in e-commerce and e-banking organizations.

The same technique, if applied to database encryption, will help government organizations counteract breach and compromise attempts on their highly sensitive data by outsiders supported by internal dishonest elements that secretly leak information.

On the other hand, business enterprises can grow much stronger defeating their competitors' data breach attempts by bribing their internal employees for leaking sensitive information such as customer identity, business secrets etc.

The Encryption Algorithm is more advanced and will be highly sought after due to its continued protection of information confidentiality even after the private key is compromised by hackers with the help of trust breachers from within the company. I call his encryption method *Absolute Public Key Cryptography*.

The above security essential is seriously lacking in the encryption techniques presently available in the market as all the existing algorithms were developed with the assumption that the enemy is sitting outside the corporate premises or network. However, today the reality is far from the assumption and this has been proved by several incidents wherein the in-house staff revealed confidential customer details to hackers. While surviving private key compromise attacks is paradoxical and impractical with other encryption techniques, my encryption makes it quite viable and a firm reality poised to save billions of Dollars lost to hackers and fraudsters every year due to data breach and identity theft.

The presently existing algorithms protect encrypted information passing across the Internet only as long as the private key is kept confidential by its owner. Once the private key is revealed, for whatever reasons, by the website or database administrators, all these algorithms remain helpless in protecting customers' confidential information or enterprise's sensitive data. This is where my encryption comes in to the picture and takes the ride.

When compared to other encryptions, my encryption technique is astronomically stronger. If the existing algorithms take a year to break on an infrastructure of several parallel gigantic supercomputers, my encryption takes several trillion years on the same infrastructure.

The encryption method employs a new concept called *Blind Encryption* wherein the original information is encrypted into two ciphers using two blind keys. The two ciphers are delivered to the receiver through two different routes over the Internet. Blind keys are unknown, randomly selected values. None of the parties – the sender, receiver, attacker and even the inventor himself - has any idea of the blind keys. The blind keys are randomly selected during runtime and cleared from the program memory once encryption is complete, leaving no record thereof for any

JILT

Certified Professional Translation

Head Office: #9-4-131/28, Tombs Road, Tolichowki, Hyderabad-500008, India, Tel: 91-406514627
Date: 26/12/2017 DOC # C00361 Website: www.jilt.co.in, e-mail: info@jilt.co.in

Authorised by: 



of the parties involved. Consequently, the encryption can be successfully decrypted only by the intended receiver. It is not possible for an adversary at an intermediary IP router intercepting a cipher to successfully decrypt the information even when he has knowledge of the private key acquired by bribing an insider.

According to an FBI report, business enterprises in U.S alone incur a yearly loss of more than US\$ 50 billion due to data breach and identity theft. In light of the above fact, my invention will be seen as a landmark in cryptography and information security, fortifying enterprise businesses against identity thieves and hackers.

- **Where do find your encryption useful?**

Entities that can benefit from the cryptographic system are business enterprises, government agencies, credit card companies, RDBMS providers, banks, payment terminals, key certifiers, business networks, hosting providers, and e-mail providers.

- **What is your ambition with this invention?**

My ambition is that the invention be useful to every stake holder in information security through out the world. In order to meet this ambition, I am trying to share this knowledge with the world through media. Also, during my leisure time, holidays and vacations, I would like to share my views and ideas with people having similar interest at cheman_shaik@rediffmail.com.



JILT

Certified Professional Translation

Head Office: #9-4-131/28, Tomba Road, Tolichowki, Hyderabad-500008, India, Tel: +91-40-6146277,
Date 26/12/2017 # C00362 website: www.jilt.co.in, e-mail: info@jilt.co.in

Authorised by: 